ORTHOGONAL F-RECTANGLES, ORTHOGONAL ARRAYS, AND CODES

by

Walter T. Federer, Cornell University

and

John P. Mandeli, Virginia Commonwealth University

BU-822-M

June 1983

Abstract

The relationships between a set of orthogonal F-squares or F-rectangles and orthogonal arrays are described. The relationship between orthogonal arrays and error-correcting codes is demonstrated. The development of complete sets of orthogonal F-rectangles allows construction of codes of any word length and for any number of words. Likewise, the development of F-rectangle theory makes code construction much more flexible in terms of a variable number of symbols. The relationship among sets of orthogonal hyperrectangles, orthogonal arrays and codes is also described.

ORTHOGONAL F-RECTANGLES, ORTHOGONAL ARRAYS, AND CODES

by

Walter T. Federer and John P. Mandeli
Cornell University — Virginia Commonwealth University

BU-822-M* June 1983

1. Introduction

Considerable theory has been developed over the last dozen years on orthogonality of F-squares and F-rectangles. Although the original work was done by Finney (1945, 1946 a,b) approximately 40 years ago, the topic of F-squares laid relatively dormant until Hedayat (1969) wrote a Ph.D. dissertation. Since that time, many papers have been published, starting with the one by Hedayat and and Seiden (1970). There were, however, two somewhat related papers in 1966 by Freeman and in 1967 by Addelman.

Orthogonal F-squares and F-rectangles can be used to generate orthogonal arrays (OAs). These OAs are distinctly different from those generated from a set of pairwise orthogonal Latin squares (POLS). The OAs obtained from a POLS set have the same number of symbols in every row (runs). By definition, the number of symbols from rows and columns of an F-square differs from the number in the F-square (FS). The resulting OAs will now have more than one set of symbols. Since the number of symbols can vary from one FS to another in an orthogonal set, OAs can be generated with several sets of symbols.

Since there is a 1 : 1 correspondence between POLS, OAs, and error-correcting codes, as described by Golomb and Posner (1964) and Federer, et al (1971), one

---

* In the Mimeo Series of the Biometrics Unit, Cornell University, Ithaca, New York.

can construct codes from OAs. The 1 : 1 correspondence between orthogonal F-squares and OAs is easily established (see Mandeli, et al., 1981, e.g.). The 1 : 1 correspondence between OAs and codes allows construction of codes with different numbers of symbols in various words or messages or in some letters of the words or messages. In addition, the construction of sets of orthogonal rectangles and hyperrectangles allows the length of the message and the number of messages to be as large as desired for certain sets of symbols. This flexibility should add considerably to the use and construction of codes.

These concepts necessitate the development of a symbolism to accommodate the above situations (see Rao, 1946, 1973). This is described in the following section. Then we describe OAs obtainable from sets of pairwise orthogonal F-squares, F-rectangles, and F-hyperrectangles. In the last section, it is shown how to obtain codes from the preceding sections. As much as possible, we use the notation and definitions given in the literature.

2. Notation and Symbolism

Let LS(v) denote a Latin square of order v and let POLS(v,t) denote a set of t pairwise orthogonal Latin squares of order v. The corresponding orthogonal array of n assemblies (columns), k runs (rows), v symbols, and of strength 2 may be denoted as $OA(n=v^2,k=t+2,v,2)$. Likewise, the corresponding notation for a block code derived from the $OA(v^2,t+2,v,2)$ is $C(v^2,t+2,v,d)$ where there are v^2 words, each of length t+2, with v symbols used for each word. Note that not all v symbols need appear in each word. Alternatively, one could have t+2 words of length v^2 which would be denoted by $C(t+2,v^2,v,d)$. The distance between words is the number of symbols by which two words differ. The minimum distance between any two words in the code is defined as Hamming distance.

To illustrate the above, the POLS(3,2) set leads to the OA(9,4,3,2) which is

Latin square	OA(9,4,3,2)		
rows	000	111	222
columns	012	012	012
Latin square one	012	120	201
Latin square two	012	201	120

If one considers the columns to be the 9 words of length 4 with v=3 symbols, the Hamming distance is d=3. If one considers the rows to be the t+2 words of length v^2=9 with v=3 symbols, the Hamming distance is d=6.

Let FS(c,λ^v), where $\lambda v=c$, denote an F-square of order c with v symbols each occurring λ times in each row and in each column; let POFS(c,λ^v,t) denote a set of pairwise orthogonal F-squares (FSs). Now, if one constructs an OA from this set, two rows of the OA will have c symbols with each symbol occurring c times, and t rows will have v symbols with each symbol occurring λc times. To illustrate, consider the particular FS($4,2^2,9$) set which produces the following OA (Note from Schwager, et al., (1983), that there are at least three non-isomorphic sets.):

0000	1111	2222	3333
0123	0123	0123	0123
1100	1100	0011	0011
1010	1010	0101	0101
1001	1001	0110	0110
1100	0011	1100	0011
1100	0011	0011	1100
1010	0101	1010	0101
1010	0101	0101	1010
1001	0110	1001	0110
1001	0110	0110	1001

The above OA is denoted by OA(16;2,9;4,2;2).

Consider now the FS$(c;\lambda_1^{\alpha_1},\cdots,\lambda_a^{\alpha_a})$, where $\Sigma_{i=1}^{a}\alpha_i = v$, $\Sigma\alpha_i\lambda_i = c$, and α_i is the number of symbols occurring λ_i times in each row and in each column. For example, for FS$(6;1^1,2^1,3^1)$ and FS$(6;1^4,2^1)$ the FSs are

a	b	b	c	c	c
b	b	c	c	c	a
b	c	c	c	a	b
c	c	c	a	b	b
c	c	a	b	b	c
c	a	b	b	c	c

and

a	b	c	d	e	e
b	c	d	e	e	a
c	d	e	e	a	b
d	e	e	a	b	c
e	e	a	b	c	d
e	a	b	c	d	e

The corresponding notation for a set of pairwise orthogonal FSs is POFS$(c;\lambda_1^{\alpha_1},\cdots,\lambda_a^{\alpha_a};t)$ when the number and frequency of symbols stays the same in each of the t FSs. However, when this number and frequency changes from FS to FS, we denote the h^{th} FS, $h=1,2,\cdots,t$, as FS$(c;\lambda_{h1}^{\alpha_{h1}},\cdots,\lambda_{a_h}^{\alpha_{a_h h}})$, where $\Sigma_{i=1}^{a_h}\alpha_{hi} = v_h$ the number of symbols in the h^{th} FS and $\Sigma_{i=1}^{a_h}\alpha_{hi}\lambda_{hi} = c$. A set of t orthogonal such FSs is denoted as $\cup_{h=1}^{t}$OFS$(c;\lambda_{h1}^{\alpha_{h1}},\cdots,\lambda_{a_h}^{\alpha_{a_h h}})$. To illustrate for c=4 and t=3, the set

FS$(4;1^4)$

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

FS$(4;1^2,2^1)$

0	1	2	2
2	2	1	0
1	0	2	2
2	2	0	1

FS$(4;1^1,3^1)$

0	1	1	1
1	1	0	1
1	1	1	0
1	0	1	1

forms a set of three pairwise orthogonal FSs with four symbols in the first FS, three symbols in the second FS, and two symbols in the third FS.

For the above situation, the corresponding OA may be denoted as OA$(c^2;2,1,1,\cdots,1;c,v_1,v_2,\cdots,v_t;2)$ where there are v_h symbols, $h=1,2,\cdots,t$, in the h^{th} FS. One row of the OA is obtained from one FS and if some of the v_h were equal, this would be reflected in the number of rows with that number of symbols.

For F-rectangles (FRs), it is necessary to denote the number of rows r in the FR as well as the number of columns c. We use the notation $FR(c,r;\lambda_1^{\alpha_1},\cdots,\lambda_a^{\alpha_a};\pi_1^{\alpha_1},\cdots,\pi_a^{\alpha_a})$ with c columns, r rows, α_i symbols occurring λ_i times in columns with $\Sigma\alpha_i\lambda_i = c$, and α_i symbols occuring π_i times in the rows with $\Sigma\alpha_i\pi_i = r$. The corresponding set of t pairwise orthogonal FRs is denoted as $\bigcup_{h=1}^{t} OFR(c,r;\lambda_{h1}^{\alpha_{h1}},\cdots,\lambda_{a_h}^{\alpha_{a_h}};\pi_{h1}^{\alpha_{h1}},\cdots,\pi_{a_h}^{\alpha_{a_h}})$. For example, an $FS(12,6;4^1,6^1,2^1;2^1,3^1,1^1)$ and an $FS(12,6;4^2,2^2;2^2,1^2)$ orthogonal pair is

0	0	1	1	1	2	0	0	1	1	1	2
2	0	0	1	1	1	2	0	0	1	1	1
1	2	0	0	1	1	1	2	0	0	1	1
1	1	2	0	0	1	1	1	2	0	0	1
1	1	1	2	0	0	1	1	1	2	0	0
0	1	1	1	2	0	0	1	1	1	2	0

0	1	2	0	1	1	2	0	3	1	3	0
1	0	1	3	1	2	1	3	0	0	2	0
3	2	1	2	0	1	0	1	0	1	0	3
2	0	3	1	3	0	0	1	2	0	1	1
1	3	0	0	2	0	1	0	1	3	1	2
0	1	0	1	0	3	3	2	1	2	0	1

The corresponding OA is:

0 0 0 0 0 0	1 1 1 1 1 1	2 2 2 2 2 2	3 3 3 3 3 3	4 4 4 4 4 4	5 5 5 5 5 5
0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5
0 2 1 1 1 0	0 0 2 1 1 1	1 0 0 2 1 1	1 1 0 0 2 1	1 1 1 0 0 2	2 1 1 1 0 0
0 1 3 2 1 0	1 0 2 0 3 1	2 1 1 3 0 0	0 3 2 1 0 1	1 1 0 3 2 0	1 2 1 0 0 3

6 6 6 6 6 6	7 7 7 7 7 7	8 8 8 8 8 8	9 9 9 9 9 9	10 10 10 10 10 10	11 11 11 11 11 11
0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5	0 1 2 3 4 5
0 2 1 1 1 0	0 0 2 1 1 1	1 0 0 2 1 1	1 1 0 0 2 1	1 1 1 0 0 2	2 1 1 1 0 0
2 1 0 0 1 3	0 3 1 1 0 2	3 0 0 2 1 1	1 0 1 0 3 2	3 2 0 1 1 0	0 0 3 1 2 1

which we denote as $OA(72;1,1,1,1;12,6,2^1{:}3^1{:}1^1,2^2{:}1^2;2)$. Here, $2:3:1$ indicates three symbols with relative frequencies 2, 3, and 1, and $2^2:1^2$ indicates four symbols with relative frequencies 2, 2, 1, and 1. In general, we denote such a derived OA as OA(cr; 1, 1, $t_1, \cdots, t_d$;c,r, $\bigcup_{h=1}^{d}[\lambda_{h1}^{\alpha_{h1}} : \lambda_{h2}^{\alpha_{h2}} : \cdots : \lambda_{a_h}^{\alpha_{a_h}}]$;2) where the relative frequencies have the smallest common denominator. Note that this relative frequency of symbols in lowest terms is the same in rows as in columns of an FR. The above OA notation can be somewhat simplified as OA(cr;$b_1, b_2, \cdots, b_a$; $s_1, s_2, \cdots, s_a$;2), where there are cr columns with b_i rows of s_i symbols, $i=1,2,\cdots,a$. This is the notation suggested by Mandeli et al. (1981). Rao (1973) uses a somewhat different notation.

Additional notation, especially for codes, will be developed as needed in the text.

3. Orthogonal Arrays Obtainable from POFSs

Hedayat (1969), Hedayat and Seiden (1970), and Hedayat, et al. (1975) have demonstrated how to construct F-squares and complete sets of F-squares of order s^m, s a prime power and m a positive integer. Since there are s^m rows, s^m columns, and $(s^m-1)^2/(s-1)$ FSs, each with s symbols, one can construct the OA(s^{2m};2,$(s^m-1)^2/(s-1)$; s^m,s;2) from the complete set of FSs. Federer (1977) constructed complete sets of FSs of order n=4t for all t for which a Hadamard matrix of side 4t exists. These can be used to construct the OA(n^2;2,$(n-1)^2$; n,2;2). Some examples are:

OA(4^2;2,9;4,2;2)	OA(16^2;2,225;16,2;2)
OA(8^2;2,49;8,2;2)	OA(25^2;2,144;25,5;2)
OA(9^2;2,32;9,3;2)	OA(27^2;2,338;27,3;2)
OA(12^2;2,121;12,2;2)	OA(28^2;2,729;28,2;2) .

Mandeli (1975) and Mandeli and Federer (1983) constructed complete sets of FSs of order s^m with varying numbers of symbols of the form $s, s^2, \cdots, s^{m-1}$,

s^m with repetitions s^{m-1}, $s^{m-2}, \cdots, s, 1$, respectively. These FSs can be used to form OAs of the form $OA(s^{2m}; n_m, n_{m-1}, \cdots, n_2, n_1; s^m, s^{m-1}, \cdots, s^2, s; 2)$ where some of the n_i, $i=1,\cdots,m$, can be zero, in which case the corresponding number of symbols s^i is deleted from the number of symbols. Examples of the above for $s^m=8$ are $POFS(8;1^8,2^4,4^2;6,1,4)$, $POFS(8;1^8,2^4,4^2;5,2,8)$, $POFS(8;1^8,2^4,4^2;7,0,0) = POFS(8;1^8;7) = POLS(8,7)$; these can be used to form the OAs as $OA(64;8,1,4;8,4,2;2)$, $OA(64;7,2,8;8,4,2;2)$ and $OA(64;9;8;2)$. Many sets of this form are possible, of which the above sets are specific examples.

Mandeli, et al. (1981) gave the following theorem:

If the orthogonal array $(n,k,s,2)$ and a POLS(s,t) exists, then there exists an orthogonal array $(n^2, tk^2+2, s, 2)$.

From this result, an $OA(n^2;2,tk^2+2;n,s;2)$ exists. They showed that for $n=2s^p$ such an orthogonal array can be constructed.

Schwager, et al. (1983) constructed complete sets of FSs of order 2^n of the form $POFS(2^n;1^{2^n},(2^{n-1})^2;1,(2^n-1)(2^n-2))$. These can be used to construct the $OA(2^{2n};3,(2^n-1)(2^n-2);2^n,2;2)$. They showed how to construct two nonisomorphic sets of these FSs and both of these are nonisomorphic to those constructed by Hedayat, et al. (1975) and by Federer (1977). Thus, three sets of nonisomorphic OAs are obtainable from FSs of order 2^n.

Schwager, et al. (1983) used Hall's (1961) nonisomorphic Hadamard matrices of side 16 to form three nonisomorphic FSs of order four. These $POFS(4;2^2;9)$ can be used to form the $OA(16;2,9;4,2;2)$.

Another special case has been described for FSs of order six. Hedayat, et al. (1975) gave the $POFS(6;2^3;4)$; Anderson, et al. (1974) constructed the

POFS$(6;2^3;8)$ and showed it could not be extended. Federer (1975) constructed the POFS$(6;3^2,2^3;1,8)$ and the POFS$(6;1^6,2^3;1,7)$ sets. Finney (1982) gave constructions for POFS$(6;1^6,2^3;1,7)$, POFS$(6;1^6,3^2;1,8)$, and POFS$(6;1^6,3^2;1,10)$; he stated that no pair of orthogonal FSs exists for five symbols or for four symbols composed of two in once and two in twice in each row and column.

The above illustrations are summed up in the following theorem:

<u>Theorem 3.1</u>. <u>The existence of a set of</u> POFS$(n;\lambda^v;t) \Leftrightarrow$ OA$(n^2;2,2\ell+t;n,v;2)$,

$$\text{where } \ell = \begin{cases} \ell' > 1 \text{ if an OA}(n,\ell',v,2) \text{ exists} \\ 1 \quad \text{otherwise} \end{cases} .$$

<u>Proof</u>: <u>Case I</u>. Suppose an OA$(n,\ell',v,2)$ does <u>not</u> exist. Let R be the following $n \times n$ matrix:

$$R = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ v-1 & v-1 & \cdots & v-1 \\ 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ v-1 & v-1 & \cdots & v-1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ v-1 & v-1 & \cdots & v-1 \end{bmatrix} .$$

Let C be the following $n \times n$ matrix:

$$\begin{bmatrix} 0 & 1 & \cdots & v-1 & 0 & 1 & \cdots & v-1 & \cdots & 0 & 1 & \cdots & v-1 \\ 0 & 1 & \cdots & v-1 & 0 & 1 & \cdots & v-1 & \cdots & 0 & 1 & \cdots & v-1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \cdots & v-1 & 0 & 1 & \cdots & v-1 & \cdots & 0 & 1 & \cdots & v-1 \end{bmatrix}$$

We can see that R is orthogonal to C and that R and C are orthogonal to $F_1, F_2, \cdots, F_t$. Likewise, construct the $1 \times n^2$ matrices:

$R^* = (00 \cdots 011 \cdots 1 \cdots v-1\ v-1 \cdots v-1$

$00 \cdots 011 \cdots 1 \cdots v-1\ v-1 \cdots v-1 \cdots 00 \cdots 011 \cdots 1 \cdots v-1\ v-1 \cdots v-1)$

$C^* = (01 \cdots v-1\ 01 \cdots v-1 \cdots 01 \cdots v-1$

$01 \cdots v-1\ 01 \cdots v-1 \cdots 01 \cdots v-1 \cdots 01 \cdots v-1\ 01 \cdots v-1 \cdots 01 \cdots v-1)$.

R^* is orthogonal to C^*. If the rows of each of the set of t mutually orthogonal $F(n;\lambda^v)$ squares are written consecutively so as to form a $1 \times n^2$ row matrix (as, for example, when the matrix R is transformed to R^*) we get t mutually orthogonal $1 \times n^2$ row matrices $F_1^*, F_2^*, \cdots F_t^*$. Since R and C are orthogonal to $F_1, F_2, \cdots, F_t$, we have that R^* and C^* are orthogonal to $F_1^*, F_2^*, \cdots, F_t^*$. Hence, R^*, C^*, F_1^*, F_2^*, $\cdots$, F_t^* become equivalent to a $(t+2) \times n^2$ matrix when rows are orthogonal. We therefore have constructed a $OA(n^2, t+2, v, 2)$

<u>Case II</u>. Suppose now that an $OA(n, \ell', v, 2)$ does exist. Let

$$A = OA(n, \ell', m, 2)$$

$$= \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{\ell'1} & a_{\ell'2} & \cdots & a_{\ell'n} \end{bmatrix}$$

where $a_{ij} \in \{0,1,\cdots,v-1\}$ for $i=1,\cdots,\ell'$

$j=1,\cdots,n$.

Form the following $n \times n$ matrices:

$$R_i = \begin{bmatrix} a_{i1} & a_{i1} & \cdots & a_{i1} \\ a_{i2} & a_{i2} & \cdots & a_{i2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{in} & a_{in} & \cdots & a_{in} \end{bmatrix}$$

for $i=1,\cdots,\ell'$ and

$$C_{i'} = \begin{bmatrix} a_{i'1} & a_{i'2} & \cdots & a_{i'n} \\ a_{i'1} & a_{i'2} & \cdots & a_{i'n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i'1} & a_{i'2} & \cdots & a_{i'n} \end{bmatrix}$$

for $i'=1,\cdots,\ell'$.

It can be checked that the $2\ell'$ matrices R_i, $i=1,\cdots,\ell'$, $C_{i'}$, $i=1,\cdots,\ell'$ are mutually orthogonal. Likewise, the R_i and $C_{i'}$ are orthogonal to $F_1,F_2,\cdots,F_t$. If the rows of each R_i and $C_{i'}$ for i, $i'=1,\cdots,\ell'$ are written consecutively so as to form a $1 \times n^2$ row matrix, we get $2\ell'$ mutually orthogonal $1 \times n^2$ row matrices $R_i^*, C_{i'}^*$ for i, $i'=1,\cdots,\ell'$. Hence, $R_1^*,R_2^*,\cdots,R_{\ell'}^*$, $C_1^*,C_2^*,\cdots,C_{\ell'}^*$, $F_1^*,F_2^*,\cdots,F_t^*$ becomes equivalent to a $(2\ell+t) \times n^2$ matrix whose rows are orthogonal. We therefore have constructed an $OA(n^2,2\ell+t,v,2)$.

Given an $OA(n^2;2,2\ell+t;n,v;2)$ one may construct the $POFS(n;\lambda^V;t)$ set.

4. OAs FROM POFRs

Federer, et al. (1983) constructed sets of t pairwise orthogonal F-rectangles (POFRs) of the following form:

POFR $(2v,v;1^v,2^v;2)$ for any v,

POFR $(2pv,2qv;(2q)^v,(2p)^v;2)$ for any v,

POFR $(pv,qv;q^v,p^v;t)$ for any v for which a POLS(v,t) exists,

POFR $(4k,2;1^2,(2k)^2;4k-1)$ for all $4k$ for which a Hadamard matrix exists,

POFR $(v^n, v;1^v(v^{n-1})^v;v^n-1)$ for all prime powers v,

and

POFR $(v^n,v;1^v,(v^{n-1})^v;rt)$ for all v for which a POLS(v,r)-set and an OA$(v^n,t,v,2)$ exist.

Likewise, following the decomposition methods of Mandeli (1975, 1978), one may decompose an FR with $v=p^h$ symbols into $(p^h-1)/(p^k-1)$ FRs with p^k symbols. This is described in Theorems 7.1 and 7.2 of Federer, et al. (1983).

The above imply OAs of various natures as embodied in the following theorem:

Theorem 4.1. The existence of a set of POFR$(c,r;q^v,p^v;t)$ $\Leftrightarrow$ the following OAs OA$(c,r;1,1,t;c,r,v;2)$ for v any integer when p and q are even, any $v \neq 2,6$ when p and q are odd, and for all v when $r=v$ and $c=2v$.

Proof: The proof is by construction from a POFR set, and follows that for Theorem 3.1.

It should be noted that the OAs have many more rows than are available for OAs from POLSs or POFSs. For example, for $v=2$, no pair of orthogonal Latin squares exists. For Latin rectangles, there will be $4k-1$ POFRs for all $4k$ for which a Hadamard exists. This is a complete set. Also, no pair of Latin squares of order 6 exists. It is relatively simple to obtain orthogonal pairs of FRs with six rows and 24k columns, k=1,2,$\cdots$.

It is also interesting to note that one may construct orthogonal pairs of FRs with v/2 rows and 2v columns for all even v. For v=4p+3, p=1,2,$\cdots$, one can construct a pair of nearly orthogonal FRs with (v-1)/2 rows and 2v columns. These FRs will have the treatments of the pairs in a balanced incomplete block arrangement rather than in an orthogonal relationship. These results are described in Hedayat and Federer (1983).

5. OAs from Pairwise Orthogonal F-Hyperrectangles

Just as one can go from Latin squares to Latin cubes and hypercubes (see Federer, 1955, Ch. XV, e.g.), one can go from FSs to hyper-FSs (HFSs), and from FRs to hyper-FRs (HFRs). Then one can consider a set of t pairwise orthogonal HFSs which will be denoted as POHFSs. Cheng (1977, 1980), Mandeli (1978), and Mandeli and Federer (1983) have given constructions for POHFSs, Cheng for equal numbers of symbols in each HFS and the others when the number of symbols varies from HFS to HFS.

The following theorems summarize the results obtained by the above authors:

Theorem 5.1. (Cheng, Th. 3.1): *If v is a prime power and* $N_i=v^k$, k=1,2,$\cdots$,m, *then there exists a complete set of F-hyperrectangles of size* $N_1 \times N_2 \times \cdots \times N_m$ *with v symbols.*

Theorem 5.2. (Mandeli and Federer, Th. 2.2): *If* $v=p^h$, *where p is a prime or prime power*, h=1,2,$\cdots$, *and* $N_i=v^k$, k=1,2,$\cdots$, *then a F-hyperrectangle of size*

$\Pi_{i=1}^{m} N_i$ *with* v *symbols can be decomposed into* $(v-1)/(p^k-1)$ *pairwise orthogonal* F-*hyperrectangles of size* $\Pi_{i=1}^{m} N_i$ *and* p^k *symbols for all integers* k *which divide* h.

Theorem 5.3 (*Mandeli and Federer, Th. 2.3*): *If* $v=p^h$, *where* p *is a prime or prime power and* h *is a positive integer, and each* N_i *is a power of* v *for* $i=1,2,\cdots,m$, *then there exists a complete set* $\{F_{ij} | i=1,\cdots,u;\ j=1,2,\cdots,t_i\}$ *of* $\Sigma_{i=1}^{u} t_i$ *mutually orthogonal* F-*hyperrectangles of size* $\Pi_{i=1}^{m} N_i$ *and* v_i *symbols for* F_{ij} $(j=1,\cdots,t_i)$, *where* $u = \left[\Pi_{i=1}^{m} N_i - \Sigma_{i=1}^{m}(N_i-1) - 1\right]/(v-1)$, $t_i = (v-1)/(p^{k_i}-1)$, *and* $v_i=p^{k_i}$ *for integers* k_i *that divide* h, $i=1,\cdots,u$.

Theorem 5.4. (*Cheng, Th. 3.2*): *If there exist* $OA(N_i,t_i,v,2)$, $i=1,2,\cdots,h$, *then there exist* t *pairwise orthogonal* F-*hyperrectangles of size* $\Pi_{i=1}^{m} N_i$ *and* v *symbols where* $t = \Pi_{i=1}^{h}(t_i+1) - 1 - \Sigma_{i=1}^{h} t_i$.

Theorem 5.5. (*Mandeli and Federer, Th. 2.5:*) *If there exist* $OA(N_i,t_i,v,2)$, $i=1,2,\cdots,h$, *and* v *is a prime number, then there exist* t *pairwise orthogonal* F-hyperrectangles of size $\Pi_{i=1}^{h} N_i$ and v symbols, where $t = (v-1)^{h-1}\Pi_{i=1}^{h} t_i + (v-1)^{h-2} \sum_{1 \le i_1 < i_2 < \cdots < i_{h-1} \le h} t_{i_1} t_{i_2} \cdots t_{i_{h-1}} + \cdots + (v-1) \sum_{1 \le i_1 < i_2 \le h} t_{i_1} t_{i_2}$.

The sets of POHFRs can be used to construct OAs in the same manner as described in previous sections.

6. *Codes Obtainable from PCFRs and POHFRs*

As was noted in section 2, a block code $C(v^2,t+2,v,d)$ may be derived from the $OA(v^2,t+2,v,2)$ or from the POLS(v,t). The code will have v^2 messages of length t+2 using v symbols. Alternatively, one could have t+2 messages of length v^2. Since t is usually small relative to the number or length of the messages, one should consider ways of extending the number and length simultaneously. The results of Federer, *et al.* (1983) do precisely this. The

POFR $(v^m,v;1^v,(v^{m-1})^v$ set may be used to construct the $OA(v^{m+1};1,v^m;v^m,v;2)$ which, in turn, can be used to construct $C(v^{m+1};1,v^m;v^m,v;d)$, where there are v^{m+1} messages in which the first letter of a message contains one of v^m symbols, and the remaining v^m letters in the message may be one of v different letters and d is the average (or minimum) number of letters by which two messages differ. The following theorems and corollaries show some of these relationships. The code distance computed is the minimum distance. There could be a case for computing average distance. These details have not been worked out.

Theorem 6.1. $POFS(n;\lambda^v;t) \Leftrightarrow$ a $[n^2,v(1+2\ell+v),v,n^2(v-1)/v]$ v-ary code.

Proof: From Theorem 3.1, t orthogonal $FS(n;\lambda^v)s \Leftrightarrow OA(n^2,2\ell+t,v,2) = A$.

Let $B_{(1+2\ell+t)\times n^2} = \begin{bmatrix} O'_{1\times n^2} \\ A_{(2\ell+t)\times n^2} \end{bmatrix}$ when $O'_{1\times n^2}$ is the $1 \times n^2$ matrix of zeros.

Form $W^{(i)}_{(1+2\ell+t)\times n^2} = (i-1)\ J_{(1+2\ell+t)\times n^2} + B$ for $i=1,2,\cdots,v$, where $J_{(1+2\ell+t)\times n^2}$ is the $(1+2\ell+t)\times n^2$ matrix of ones. We will show that the v $(1+2\ell+t)$ rows of the v matrices $W^{(1)},W^{(2)},\ldots,W^{(v)}$ form the code.

Part 1: We will show that $W^{(1)}_{(1+2\ell+t)\times n^2} = B$ is a $C[n^2,1+2\ell+t,v,n^2(v-1)/v$. B forms a $C[N,M,q,d]$ where $N=n^2$ is the length of each row of B, $M=1+2\ell+t$ is the number of rows of B, and $q=v$ is the number of symbols of B. The last $2\ell+t$ rows of B are the orthogonal array A; hence, each symbol j from row i of A, $i=1,\cdots,2\ell+t$; $j=0,\cdots,v-1$ appears λ^2 times with each symbol j' from row i' of A, $i'=1,\cdots,2\ell+t$; $i\neq i'$, $j'=0,\cdots,v-1$, where $\lambda=n/v$. Hence, the pair of elements $\binom{j}{j}$ appear λ^2 times in a column for rows i and i'. Since there are v such pairs $\binom{j}{j}$, the number of times we have pairs of the form $\binom{j}{j}$ as a column for row i and i' of A is $v\lambda^2$. Hence, the number of pairs $\binom{j}{j'}$ for $j\neq j'=0,1,\cdots,v-1$ is $n^2-v\lambda^2$. So $d=n^2-v\lambda^2$. Therefore

$$d = n^2 - v\lambda^2 = n^2 - v\left(\frac{n}{m}\right)^2 = n^2 - \frac{n^2}{v} = \frac{n^2(v-1)}{v} \quad .$$

For the first row of B, which is the row $0'_{1\times n^2}$, and any other row of B, $\binom{0}{0}$ appears $n\lambda$ times. Hence, $\binom{0}{j}$ for $j=1,2,\cdots,v-1$ appears $n^2-n\lambda$ times. So, again

$$d = n^2 - n\lambda = n^2 - n\left(\frac{n}{v}\right) = n^2 - \frac{n^2}{v} = \frac{n^2(v-1)}{v} \quad .$$

Part 2: For the same reasons as in part 1, $W^{(i)}_{(1+2\ell+t)\times n^2}$ forms a $C[n^2, 1+2\ell+t, v, n^2(v-1)/v]$ for $i=2,\cdots,v$.

Part 3: We now show that

$$W = \begin{bmatrix} W^{(1)}_{(1+2\ell+t)\times n2} \\ W^{(2)}_{(1+2\ell+t)\times n^2} \\ \vdots \\ W^{(v)}_{(1+2\ell+t)\times n^2} \end{bmatrix}$$

is a $C[n^2, v(1+2\ell+t), v, n^2(v-1)/v]$. W constructs a $[N,M,q,d]$ code. Clearly,

$N = n^2$

$M = v(1+2\ell+t)$ the number of rows of W

and

$q = v.$

Let $w^{(i)}_{j(i)}$ be the j^{th} row of $W^{(i)}$ and $w^{(i')}_{j'}$ be the j'^{th} row of $W^{(i')}$.

Case I: $j = j' = 1 \Rightarrow \text{dist} = n^2$

Case II: $j \neq j'$, $j = 1 \Rightarrow \binom{i-1}{i-1}$ appears $n\lambda$ times

$$\Rightarrow \binom{i-1}{h} \text{ appears } d = \frac{n^2(v-1)}{v} \text{ times for } h=0,1,\cdots,i-2,i,\cdots,v-1$$

$$\Rightarrow \text{dist} = \frac{n^2(v-1)}{v} .$$

Case III: $j \neq j'$, $j' = 1$ similar to Case II.

Case IV: $j \neq j'$, $j, j' \neq 1 \Rightarrow \text{dist} = \dfrac{n^2(v-1)}{v}$ because these rows of W are constructed from the orthogonal array A.

Case V: $j = j'$, $j, j' \neq 1 \Rightarrow w^{(i)}_{j(i')} = (i-1)\mathbf{1}' + a_j$

$$w_j \quad = (i'-1)\mathbf{1}' + a_j$$

where $\mathbf{1}' = (1 \; 1 \; \cdots \; 1)_{1\times n^2}$ and a_j is the j^{th} row of A.

$\Rightarrow \binom{h}{h}$ does not appear for $h=0,1,\cdots,v-1$

and

$\binom{h}{h'}$ appears $n\lambda$ times for $h=0,1,\cdots,v-1$

and $h'=(i-1)+h$.

The number of such $\binom{h}{h'}$ is v. Hence, distance $= v(n\lambda) = v \cdot n \cdot \frac{n}{v} = n^2$.

Conclusion,

$$\text{Case I} \rightarrow \text{Case V} \Rightarrow d = \min\left[n^2, \frac{n^2(v-1)}{v}\right]$$

$$= \frac{n^2(v-1)}{v} .$$

Given $C[n^2, v(1+2\ell+v), v, n^2(v-1)/v]$, a PCFS$(n;\lambda^v;t)$ set is obtained by construction; hence, the other part of the implication.

Example 6.1: Using the 8 orthogonal $F(6;2^3)$ squares of Anderson, et al. (1974) we can construct a 3-ary code:

$C[6^2,3(1+2+8),3,6^2(3-1)/3] = C[36,33,3,24]$.

0'	000000	000000	000000	000000	000000	000000
R	000000	111111	222222	000000	111111	222222
C	012012	012012	012012	012012	012012	012012
$F_1 \to F_8$	120120	201201	201201	012012	012012	120120
	201201	120120	012012	012012	201201	120120
	201201	201201	120120	012012	120120	012012
	120120	012012	120120	012012	201201	201201
	122001	220011	200112	001122	011220	112200
	210021	202110	101022	021210	110202	022101
	221010	100212	021102	010221	212100	102021
	101022	021210	110202	022101	210021	202110
0'+1'	111111	111111	111111	111111	111111	111111
R + 1'	111111	222222	000000	111111	222222	000000
C + 1'	120120	120120	120120	120120	120120	120120
$F_1+1' \to F_8+1'$	201201	012012	012012	120120	120120	201201
	012012	201201	120120	120120	012012	201201
	012012	012012	201201	120120	201201	120120
	201201	120120	201201	120120	012012	012012
	200112	001122	011220	112200	122001	220011
	021102	010221	212100	102102	221010	100212
	002121	211020	102210	121002	020211	210210
	212100	102021	221010	100212	021102	010221
0'+21'	222222	222222	222222	222222	222222	222222
R+21'	222222	000000	111111	222222	111111	000000
C+21'	201201	201201	201201	201201	201201	201201
$F_1+21' \to F_8+21'$	012012	120120	120120	201201	201201	012012
	120120	012012	201201	201201	120120	012012
	120120	120120	012012	201201	012012	201201
	012012	201201	012012	201201	120120	120120
	011220	112200	122001	220011	200112	001122
	102210	121002	020211	210210	002121	211020
	110202	022101	210021	202110	101022	021021
	020211	210102	002121	211020	102210	121002

Corollary 6.1.

Corollary 6.2.

$$POFS(n;(n/s)^s;2t+kt^2) \Rightarrow OA(n^2;2t+kt^2,s,2)$$

$$\Rightarrow \left[n^2, s(1+2t+kt^2), s, \frac{n^2(s-1)}{s}\right]$$

s-ary code.

Corollary 6.3. There exists a set of $(s-1)[2(s^p-1)/(s-1)-1]^2$ orthogonal $FS[2s^p;(2s^{p-1})^s]s$, for s a prime or prime power and p a positive integer

$$\Rightarrow OA[4s^{2p}, 2\{2(s^p-1)/(s-1)-1\} + (s-1)\{2(s^p-1)/(s-1)-1\}, s, 2]$$

$$\Rightarrow \left[4s^{2p}, s(1+2\{2(s^p-1)/(s-1)-1\} + (s-1)\{2(s^p-1)/(s-1)-1\}^2), s, \frac{4s^{2p}(s-1)}{s}\right]$$

s-ary code.

Corollary 6.4. If we let the prime decomposition of a number n be $n=p_1^{\ell_1}, p_2^{\ell_2}, \cdots, p_m^{\ell_m}$, and, without loss of generality, let $p_1^{\ell_1} < p_2^{\ell_2} < \cdots < p_m^{\ell_m}$ then there exists a set of $(p_m^{\ell_m}-1)$ mutually orthogonal $F[n;(p_1^{\ell_1}, p_2^{\ell_2}, \cdots, p_{m-1}^{\ell_{m-1}})^{p_m^{\ell_m}}]$ squares.

$$\Rightarrow OA[n^2, 2+p_m^{\ell_m}-1, p_m^{\ell_m}, 2]$$

$$\Rightarrow \left[n^2, p_m^{\ell_m}(1+2+p_m^{\ell_m}-1), p_m^{\ell_m}, \frac{n^2(p_m^{\ell_m}-1)}{p_m^{\ell_m}}\right]$$

$p_m^{\ell_m}$-ary code,

i.e.,

$$\left[n^2, p_m^{\ell_m}(2+p_m^{\ell_m}), p_m^{\ell_m}, \frac{n^2(p_m^{\ell_m}-1)}{p_m^{\ell_m}}\right]$$

$p_m^{\ell_m}$-ary code.

Theorem 6.2. t orthogonal $n_1 \times n_2 \times \cdots \times n_a$ F-hyperrectangles with v symbols

$$\Leftrightarrow OA(\Pi_{i=1}^{a} n_i, \Sigma_{i=1}^{a} d_i + t, v, 2) \text{ where } \ell_i = \begin{cases} \ell_i' > 1 & \text{if a } OA(n_i, \ell_i', v, 2) \text{ exists for } i=1,2,\cdots,a \\ 1 & \text{otherwise} \end{cases}$$

$$\Leftrightarrow \left[\Pi_{i=1}^{a} n_i, v(1+\Sigma_{i=1}^{a} \ell_i + t), v, (\Pi_{i=1}^{a} n_i) \frac{(v-1)}{v}\right]$$

v-ary code.

Proof: The proof is a generalization of Theorems 3.1 and 6.1.

Corollary 6.5. If there exist orthogonal arrays $OA(N_i, n_i, s, 2)$ for $i=1,\cdots,k$ and s is a prime number $\Rightarrow$ there exist t mutually orthogonal F-hyperrectangles of size $N_1 \times N_2 \times \cdots \times N_k$ and s symbols, where

$$t = (s-1)^{k-1} n_1 n_2 \cdots n_k + (s-1)^{k-2} \sum_{1 \le i_1 < i_2 < \cdots < i_{k-1} \le k} n_{i_1} n_{i_2} \cdots n_{i_{k-1}}$$

$$+ \cdots + (s-1) \sum_{1 \le i_1 < i_2 \le k} n_{i_1} n_{i_2}$$

$$\Leftrightarrow \left[\Pi_{i=1}^{k} N_i, s(1 + \Sigma_{i=1}^{k} n_i + t), s, (\Pi_{i=1}^{k} N_i) \frac{(s-1)}{s}\right]$$

s-ary code.

7. Literature Cited

Addelmann, S. (1967). Equal and proportional frequency squares. J. Amer. Stat. Assoc. 62:226-240.

Anderson, D. A., W. T. Federer and E. Seiden (1974). On the construction of orthogonal F(2k,2)-squares. No. BU-500-M in the Mimeo Series of the Biometrics Unit, Cornell University, February.

Cheng, C.-S. (1977). Optimal designs for the elimination of heterogeneity. Ph.D. Thesis, Cornell University.

Cheng, C.-S. (1980). Orthogonal arrays with variable numbers of symbols. Annals of Stat. 8:447-453.

Federer, W. T. (1955). Experimental Design – Theory and Application. Macmillan, New York. (Republished by Oxford and IBH Publishing Co., New Delhi, 1967, 1974.)

Federer, W. T. (1975). On the construction of F-squares and single degree-of-freedom contrasts (preliminary). No. BU-566-M in the Mimeo Series of the Biometrics Unit, Cornell University, August.

Federer, W. T. (1977). On the existence and construction of a complete set of orthogonal F(4t;2t,2t)-squares design. Annals of Stat. 5:561-564.

Federer, W. T., A. Hedayat, E. T. Parker, B. L. Raktoe, E. Seiden and R. J. Turyn (1971). Some techniques for constructing mutually orthogonal Latin squares. MRC Tech. Summary Report No. 1030, June. (Preliminary version published in Proc. 15th Conf. Design Expts. Army Res. Development and Testing, ARO-D70-2, pp. 673-796.)

Finney, D. J. (1945). Some orthogonal properties of the 4 x 4 and 6 x 6 Latin squares. Annals Eugenics 12:213-219.

Finney, D. J. (1946a). Orthogonal partitions of the 5 x 5 Latin squares. Annals Eugenics 13:1-3.

Finney, D. J. (1946b). Orthogonal partitions of the 6 x 6 Latin squares. Annals Eugenics 13:184-196.

Finney, D. J. (1982). Some enumerations for the 6 x 6 Latin squares. Utilitas Mathematica 21(A):137-153.

Freeman, G. H. (1966). Some non-orthogonal partition of 4 x 4, 5 x 5, and 6 x 6 latin squares. Annals Math. Stat. 37:661-681.

Golomb, S. W. and E. C. Posner (1964). Rook domains, Latin squares, affine planes, and error-distributing codes. IEEE Transactions on Information Theory IT-10, 196-208.

Hall, M., Jr. (1961). Hadamard matrices of order 16. Jet Propulsion Lab. Research Summary 36-10, 1, 21-26, J. P. L. Pasadena, California.

Hedayat, A. (1969). On the theory of the existence, non-existence, and the construction of mutually orthogonal F-squares and Latin squares. Ph.D. Thesis, Cornell University.

Hedayat, A. and W. T. Federer (1983). Orthogonal F-rectangles for all even v. BU-819-M in the Mimeo Series of the Biometrics Unit, Cornell University, June.

Hedayat, A., D. Raghavarao and E. Seiden (1975). Further contributions to the theory of F-squares design. Annals Stat. 3:712-716.

Hedayat, A. and E. Seiden (1970). F-square and orthogonal F-square designs: A generalization of Latin square and orthogonal Latin square design. Annals Math. Stat. 41:2035-2044.

Mandeli, J. P. (1975). Complete sets of orthogonal F-squares. M.S. Thesis, Cornell University.

Mandeli, J. P. (1978). Contributions to the theory of F-square and F-cube designs. Ph.D. Thesis, Cornell University.

Mandeli, J. P. and W. T. Federer (1983). On the construction of mutually orthogonal F-hyperrectangles. Utilitas Mathematica (accepted for publication).

Mandeli, J. P., F.-C. H. Lee and W. T. Federer (1981). On the construction of orthogonal F-squares of order n from an orthogonal array (n,k,s,2) and an OL(s,t) set. J. Stat. Plan. and Infer. 5:267-272.

Rao, C. R. (1946). Hypercubes of strength d leading to confounded designs in factorial experiments. Bull. Calcutta Math. Soc. 38;67-78.

Rao, C. R. (1973). Some combinatorial problems of arrays and applications to design of experiments. In A Survey of Combinatorial Theory (J. N. Srivastava, ed.), pp. 349-359. North-Holdand, Amsterdam.

Schwager, S. J., W. T. Federer and J. P. Mandeli (1983). Embedding cyclic Latin squares of order 2^n in a complete set of orthogonal F-squares. BU-788-M in the Mimeo Series of the Biometrics Unit, Cornell University (accepted for publication in the J. Stat. Plan. and Infer.).

Schwager, S. J., W. T. Federer and B. L. Raktoe (1983). Nonisomorphic complete sets of orthogonal F-squares, Hadamard matrices, and decompositions of a 2^4 design. BU-807-M in the Mimeo Series of the Biometrics Unit, Cornell University, February.